Clapotis: Evaluating the isogeny class group action in polynomial time

AUREL PAGE AND DAMIEN ROBERT

Abstract. Let $E/\mathbb{F}_q$ be an elliptic curve with an effective primitive orientation by a quadratic imaginary order $R \subset \mathrm{End}(E)$. Let $\mathfrak{a}$ be an invertible ideal in R. We give a polynomial time algorithm in $O(\log^{O(1)}(\Delta_R))$ arithmetic operations over $\mathbb{F}_q$ to compute the class group action $E \mapsto E_{\mathfrak{a}} \simeq E/E[\mathfrak{a}]$.

1. Introduction

1.1. **Class group action in isogeny based cryptography.** Since quantum computers threaten cryptography based on the discrete logarithm problem (DLP), cryptography based on an effective group action has gained spotlight in post-quantum cryptography. Indeed, many algorithms translate from the DLP setting to the group action setting, which allows one to get a post-quantum version.

Isogeny based group actions are convenient ways to instantiate group actions in practice. In this case the group is a class group acting on suitable elliptic curves over a finite field. However, a big drawback of isogeny based group action is that it only naturally allows us to compute a restricted group action: i.e., the action of "small" generators with "small" exponents.

This is a problem for many protocols based on group actions, which need the full group action rather than the restricted group action. Up to now the only solution to get an unrestricted group action in the isogeny setting was to compute a lattice of relations in the class group, and replace the action of an ideal $\mathfrak{a}$ by the action of an equivalent and sufficiently small ideal $\mathfrak{b}$.

This is done in two step.

(1) First there is an offline phase which takes a generating set of small prime ideals and computes the lattice of relations. Then a nice basis of the relation lattice is computed.
(2) Then in the online phase, a closest vector problem (CVP) is solved to reduce the ideal $\mathfrak{a}$ to an equivalent nice ideal $\mathfrak{b}$.

Such a computation for CSDIH-512 was done in [BKV19].

In a generic class group, computing the lattice of relation takes subexponential classical time or quantum polynomial time (all our complexity will be expressed by default in terms of the logarithm of the discriminant). One solution to this problem is to instead work in a non maximal order of large conductor inside a maximal order of small discriminant. Finding the lattice of relations then reduces to solving the DLP in the multiplicative group of a finite field, which is easier than the general case ([FFK+23]), and can even be solved in polynomial time if the corresponding multiplicative group is sufficiently smooth [CL23].

The second problem is that to get a solution of CVP of good quality (ie a polynomial time approximation factor), one needs a good basis of the lattice. It is currently not known how to exploit the fact that the lattice is a lattice of relations in a class group, and the best algorithm is a generic lattice algorithm that takes exponential time (even with a quantum algorithm). In practice, at the current level of security the lattice reduction step is not the bottleneck compared to finding the lattice of relations, but asymptotically this exponential offline computation will become infeasible. Currently the best we can do asymptotically is spend a subexponential time to obtain a better basis, allowing for a subexponential approximation factor; computing the corresponding isogeny action will then take subexponential time

Date: November 19, 2024.
2010 *Mathematics Subject Classification.* Primary... Secondary...
Key words and phrases. Keywords: isogenies, group action.
Ciao.

too. In https://yx7.cc/blah/2023-04-14.html, Panny argues that this step can be (heuristically) made classically in $L(1/3)$ (in contrast to the $L(1/2)$ quantum Kuperberg's attack).

So currently there are no asymptotically polynomial time instance of an unrestricted group action, even for specific suborders.

1.2. **An equivalence of categories in higher dimension.** In this paper, we describe Clapotis: CLass group Action in POlynomial TIme via Sesquilinear forms. Clapotis is a polynomial time algorithm that, given an elliptic curve $E/\mathbb{F}_q$ (supersingular or ordinary) oriented by a quadratic imaginary order R (with an effective action) and an invertible ideal $\mathfrak{a}$, compute the group action of $\mathfrak{a}$ on E. There are no restrictions on the order, and in particular our algorithm applies to CSIDH [CLMPR18].

We recall that if E is oriented by R, and $\mathfrak{a}$ is an invertible ideal, then the action is given by $\mathfrak{a} \cdot E = E/E[\mathfrak{a}]$. We use the now standard trick of going to higher dimension. We will describe two variants of our polynomial time group action algorithm.

In the first variant, we use the fact that Kani's lemma can be used to efficiently split a N_1N_2-isogeny into a N_1-isogeny followed by a N_2-isogeny, see the survey [Rob24b] for more details. We then construct a suitable N_1N_2-endomorphism γ on E, such that splitting it as above recovers $\mathfrak{a} \cdot E$. We call this variant Clapoti (CLass group Action in POlynomial TIme), it has already been published in the note [PR23], and we recall how it works in the appendix. This variant can be seen as a generalisation of the QFesta trick from [NO23]. In QFesta, they build an appropriate $q(2^m - q)$ endomorphism in order to efficiently generate a q-isogeny starting from E_0. What we did in [PR23], is first, to extend the QFesta algorithm into a general splitting algorithm on any N-isogeny, relaxing in particular the degrees condition on N to simply $N = N_1N_2$ with N_1 and N_2 being coprime. Secondly, we explained how to build an appropriate endomorphism on E whose splitting would give $E \to \mathfrak{a}E$ rather than a random isogeny.

Our second variant is more reminiscent of the KLPT smoothening algorithm. Indeed, in that variant we explain how we can smoothen the two-dimensional $N(\mathfrak{a})$-isogeny $E^2 \to \mathfrak{a}E \oplus \overline{\mathfrak{a}}E$ into an equivalent but smooth isogeny.

For our smoothening algorithm, we need to have a good description of all isogenies starting from E^2. In this paper, we generalise this to a description of all isogenies starting from a power E^g of E. We prove that there is an equivalence of categories between (the opposite category of) unimodular Hermitian R-modules and the category of R-oriented principally polarised abelian varieties isogenous to E^m with isogenies respecting the orientation (and some extra condition when p is inert in R, see Section 2 for more details). This equivalence of categories is an extension of the work of [JKP+18] (see also [Wat69; Kan11; KNRR21]) from the non oriented case to the oriented case.

Via this equivalence of categories we can translate our isogeny problem into a linear algebra question. The isogeny $E \to E/E[\mathfrak{a}]$ corresponds to the inclusion $\mathfrak{a} \to R$. Instead of computing this isogeny, we find a different isogeny in dimension two, corresponding on the Hermitian side to a module map $F\colon \mathfrak{a} \oplus \overline{\mathfrak{a}} \to R \oplus R$ which is an N-similitude, with N nice (for instance, powersmooth). Translating back to the algebraic side, this map corresponds to an N-isogeny $E^2 \to E/E[\mathfrak{a}] \times E/E[\overline{\mathfrak{a}}]$, which we can evaluate efficiently if N is nice enough. We then use pairings to distinguish between $E/E[\mathfrak{a}]$ and $E/E[\overline{\mathfrak{a}}]$.

Going to dimension two allows us to solve a smoothening problem for modules of rank 2 rather than modules of rank 1, and since the similitude group GU_2 is much larger than GU_1 this opens up a lot more possibilities than trying to smoothen ideals. In fact, we are even able to directly use a variant of the KLPT algorithm [KLPT14] thanks to an exceptional isomorphism, the algebraic version of the classical isomorphism identifying $\mathrm{SU}_2(\mathbb{C})$ with the group of Hamiltonian quaternions of norm 1. More precisely, we construct an embedding $B^\times \subset \mathrm{GU}_2$ for a suitable quaternion algebra B. This allows us to apply the usual toolbox for smoothening ideals in quaternion algebras to the setting of oriented abelian surfaces. Dimension 2 is therefore already enough to find a nice powersmooth N-isogeny F with $N = O(\Delta^3)$. Our evaluation of $E/E[\mathfrak{a}]$ thus only requires the evaluation of a dimension 2 isogeny.

In summary, our contributions consist on generalising the usual equivalence of category between isogenies and ideals from dimension 1 to higher dimension, and then deriving a version of the KLPT algorithm from dimension 1 in the supersingular case to dimension 2 for the oriented case.

1.3. **Outline.** Let $E/\mathbb{F}_q$ be a primitively oriented curve by a quadratic imaginary order R. In Section 2 we describe the equivalence of categories between unimodular R-modules and similitudes on one hand, and oriented abelian varieties isogenous to E^n and oriented isogenies on the other hand. Then in Section 3, we explain how to compute this equivalence in practice, notably how to convert a similitude into an isogeny. Our goal to compute the class group action corresponding to an ideal $\mathfrak{a}$ is to find a nice similitude $\mathfrak{a} \oplus \overline{\mathfrak{a}} \to R^2$ corresponding to a dimension 2 isogeny $E^2 \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$. In Section 4 we describe an exceptional isomorphism which allows us to reduce to a similar problem for a quaternionic ideal, a problem that has received ample attention in the literature to make the Deuring correspondence ideal effective. Then, in Section 5, we translate back from the quaternionic world to rank 2 R-Hermitian modules to compute our group action. In Section 6 we give some applications of our algorithm, and conclude with some perspectives in Section 7.

1.4. **History of the paper.** It all started with a question by Antonio Sanso in October 04 2023 to the second author, on whether we could extend the QFesta trick to compute class group actions. Intrigued, the second author tried to extend the QFesta ideas to build an isogeny $E^2 \to (\mathfrak{a} \cdot E)^2$, but did not succeed. As a fallback, he instead considered the strategy of generalizing the KLPT algorithm from supersingular curves in dimension 1 to oriented elliptic curve products in dimension 2. Indeed, he knew from [KNRR21] that, there was a nice equivalence of categories[1] with Hermitian modules, which allowed one to replace the question of smoothening an isogeny with the question of smoothening an Hermitian similitude. Now, reasoning in terms of the quadratic form induced by the Hermitian form, the hope was that moving from dimension 1 to dimension 2, i.e. a rank 2 quadratic form over $\mathbb{Z}$ to a rank 4 quadratic form, would make the smoothening problem much easier. Indeed, while finding a smooth equivalent R-ideal to $\mathfrak{a}$ is hard (it takes subexponential time), the equivalent problem for ideals in a quaternion order (so with a rank 4 quadratic form) had been solved heuristically by the KLPT algorithm [KLPT14], and under GRH in [Wes22].

At that point, he enlisted the help of the first author, a specialist in quaternion algebras. The first author was quick to point out that there was more than just an analogy between the smoothening problem in rank 2 and the ideal smoothening problem for a quaternion algebra, more than just the fact they were given by rank 4 quadratic forms. As explained above there is an exceptional isomorphism $B^\times \to \mathrm{GU}_2$, which translated from number fields to orders would allow to directly reduce[2] to KLPT. Working out this isomorphism explicitly (see Section 4), he showed that the correct isogeny to smoothen was $E^2 \to \mathfrak{a} \cdot E \oplus \overline{\mathfrak{a}} \cdot E$; because there was a direct translation into the quaternionic world. Implementing the algorithm in Pari/GP, he had a working cryptographic size example of smoothening on October 26 2023.

At that point, we had a first preliminary version of the current paper, with the proof of the equivalence of categories, the reduction to KLPT, and a working example. Now the isogeny $E^2 \to \mathfrak{a} \cdot E \oplus \overline{\mathfrak{a}} \cdot E$ we had built is an isogeny between a product of elliptic curves, and the converse of Kani's lemma implies that it comes from an isogeny diamond. In October 30 2023, in order to explain why Kani's lemma would not help this time and we really needed the full power of the module equivalence of categories, the second author worked out the corresponding isogeny diamond (see Example 5.5). He found out that the contrary was true: in fact, we can use Kani's lemma as a powerful tool to split an N_1N_2-isogeny, with N_1 coprime to N_2, into a N_1-isogeny followed by a N_2-isogeny. This involves computing a $N_1 + N_2$-isogeny in dimension 2, so is only efficient when $N_1 + N_2$ is smooth. But the general case is easily handled, the trick, which he had already used in [Rob23] following the ideas of [CD23; MMPPW23], is simply to pad the N_1 and N_2 isogenies with u and v-isogenies (or simply endomorphisms), with u, v chosen such that $uN_1 + vN_2$ is smooth. As explained in [Rob23], such an u-endomorphism can always be constructed, replacing E by E^4 if needed. The argument was written in October 31 in the short note [PR23], introducing the Clapoti algorithm, giving a polynomial algorithm to compute the group action, while completely bypassing the module equivalence of categories.

Now, Clapoti is, *a posteriori*, an "obvious" generalisation of the QFesta algorithm. So in retrospect, Antonio Sanso was completely right in his intuition that the QFesta approach could apply to the class

[1] At least for the Frobenius orientation, but it was clear that it would be easy to extend it to the oriented case.

[2] Reducing to an already solved problem, a well known mathematical trick!

group action. However, as the above history shows, this is not at all how we obtained it. In particular, the crucial observation, due to the first author, that we should consider $\mathfrak{a} \cdot E \oplus \overline{\mathfrak{a}} \cdot E$ rather than $(\mathfrak{a} \cdot E)^2$ was obtained from the equivalence of category combined with the special isomorphism mentioned above.

As a side effect of the publication of [PR23] in November 2023, the current article (describing our second variant Clapotis) remained unfinished. Part of the reason is that the second author was busy applying the ideas of Clapoti to the supersingular case to construct SQISign2d [BDD+24]. The existence of this draft was however made clear in [PR23], and the authors shared widely upon request. As an unfortunate side effect of this delay, other researchers rediscovered (via a more *ad hoc* approach compared to our more conceptual point of view) that the smoothening problem inherent in Clapotis could reduce to the KLPT algorithm.

Although our main motivation for the original article, namely computing class group action in polynomial time, was solved in [PR23], we still feel it is important to publish the full version of the algorithm.

(1) First, the equivalence of categories, which allows us to recast isogeny problems involving abelian varieties isogenous to E^g into module problems, will certainly prove crucial in the recent trend of moving away from dimension 1 to higher dimensions in isogeny based cryptography, and notably to move beyond Kani's lemma.

    Even in dimension 1, as argued by the second author in his talk [Rob24a] at the Leuven Isogeny Days 5, the module point of view is often more convenient than the ideal point of view, notably to deal with level structure. It his also a fun exercice to translate the usual concepts from isogeny based cryptography in the module world, see the talk mentioned above for some examples.

    Recently, the second author also introduced a new module action on abelian variety, which generalises the classical ideal action on elliptic curves. The construction of this module action makes crucial use of the equivalence of categories.

(2) The exceptional isomorphism we mentioned above gives a systematic way to apply existing tools from supersingular elliptic curves to ordinary elliptic curves (by moving to dimension 2). Again, we feel that our presentation of this fact will give a deeper understanding of the relationship between these two elliptic curve worlds.

1.5. **Thanks.** The second author thanks Lorenz Panny for useful discussions on class group computations. He also gives special thanks to Antonio Sanso, who, as explained above, spurred this project by asking if the methods of QFesta [NO23] could help in computing the class group action.

2. The equivalence of categories

Following the seminal work of Deuring, the link between isogenies and ideals, or more generally module maps and isogenies, has been amply studied in the literature. See for instance [Wat69; Kan11; JKP+18] and the references in [KNRR21, § 1]. For our application, we only need the fact that a Hermitian unimodular R-module gives a principally polarised abelian variety, and that a N-similitude gives an N-isogeny, which is the easy part of the correspondence (see Theorem 2.11).

In this section, since it can be interesting for other applications, we prove the equivalence of categories in greater generality that what we need. We rely on [JKP+18] (which uses [Kan11]), which proves an equivalence of categories for non oriented isogenies; it suffices to adapt their proof to the oriented case.

Definition 2.1. Let A/k be an abelian variety over a field. Let R be a ring. An orientation of A by R is an embedding $i_A \colon R \to \mathrm{End}_k(A)$. The orientation is said to be primitive if $i_A(R)$ is saturated in $\mathrm{End}_k(A)$.

An R-oriented isogeny $f \colon A_1 \to A_2$ between two R-oriented abelian varieties is an isogeny which commutes with the orientation: if $\gamma \in R$, $f \circ i_{A_1}(\gamma) = i_{A_2}(\gamma) \circ f$. We denote by $\mathrm{Hom}_R(A_1, A_2)$ the abelian group of oriented isogenies.

Remark 2.2.

- If $f\colon A_1 \to A_2$ is an R-oriented isogeny, then $\operatorname{Ker} f$ is stable by R. Conversely, if K is a finite subgroup scheme of A_1 stable by R, then by the universal property of the quotient $A_2 = A_1/K$ there is a unique R-orientation on A_2 making the natural map $A_1 \to A_2$ R-oriented.
- If R is a quadratic imaginary order, and $E/\mathbb{F}_q$ is an R-primitively oriented elliptic curve over a finite field, then $\operatorname{Hom}_R(E,E) = R$. Indeed, $\operatorname{End}(E) \coloneqq \operatorname{End}_{\overline{\mathbb{F}}_q}(E)$ is of rank 2 or 4, and in both cases $R \subset \operatorname{End}(E)$ is its own centralizer (since it is saturated in $\operatorname{End}(E)$).

Definition 2.3. Let E/k be an R-oriented elliptic curve and M a finitely presented (f.p. in the sequel) R-module. Let $R^m \to R^n \to M \to 0$ be a presentation of M. The morphism $R^m \to R^n$ is represented by an induced matrix X acting by right multiplication. This matrix defines, by left multiplication, a morphism $X\colon E^n \to E^m$. We define $\mathcal{HOM}_R(M,E)$ to be the kernel of this map. (The same construction holds to define $\mathcal{HOM}_R(M,E)$ when E/k is any proper group scheme with an action by R).

Theorem 2.4. *Assume that R is a primitive orientation of E/k.*

(1) The construction above defines a contravariant exact functor $\mathcal{HOM}_R(\cdot,E)$ from finitely presented R-modules to proper group schemes over k. In particular, the isomorphism class of $\mathcal{HOM}_R(M,E)$ does not depend on the presentation.

(2) If k' is a k-algebra, and $A = \mathcal{HOM}_R(M,E)$, then $A(R) \simeq \operatorname{Hom}_R(M, E(k'))$. [Aurel : Je ne comprends pas, c'est quoi $A(R)$? Est-ce que c'est une typo pour $A(k')$?]

(3) If T is a R-module which is finite (as a set), then $\mathcal{HOM}_R(T,E)$ is a finite group scheme of degree $\#T^{2/\operatorname{rank} R}$.

(4) If R is a primitive [Aurel : redondant : tu as supposé primitif dans tout le théorème] orientation and M is torsion-free, then $\mathcal{HOM}_R(M,E)$ is an abelian variety isogenous to E^m where m is the R-rank of M. We have $A[n] \simeq \mathcal{HOM}_R(M, E[n])$ and $T_\ell(A) \simeq \operatorname{Hom}_R(M, T_\ell E)$ for every prime $\ell \neq p$.

(5) If $\mathfrak{a}$ is a non zero left R-ideal, then $\mathcal{HOM}_R(R/\mathfrak{a}, E) \simeq E[\mathfrak{a}]$ and $\mathcal{HOM}_R(\mathfrak{a}, E) \simeq E/E[\mathfrak{a}]$.

Proof. This is [JKP+18, Proposition 4.2 and Theorem 4.4]. □

Now let's assume that R is a quadratic imaginary order.

Lemma 2.5. *Let M be a f.p. torsion free R-module. Then there is a decomposition $M = I_1 \oplus I_2 \oplus \cdots I_m$, such that $O(I_1) \subset O(I_2) \subset \cdots \subset O(I_m)$ (hence I_i is invertible in $O(I_i)$). Furthermore, the isomorphism class of M only depends on the $O(I_i)$ and on the class of $I_1 \cdot I_2 \ldots I_m$, which is an invertible $O(I_m)$-ideal.*

Proof. This follows from the fact that a quadratic ring is a Bass order, see [JKP+18, Theorem 3.2]. □

Lemma 2.6. *If $E/\mathbb{F}_q$ admits a primitive orientation by a quadratic imaginary order R, then E is ordinary if and only if p is split in R, and E is supersingular if and only if p is ramified or inert. There is no primitive orientation by an order of conductor divisible by p.*

Proof. If $E/\mathbb{F}_q$ is ordinary, by Deuring, $\operatorname{End}_{\mathbb{F}_q}(E) = \operatorname{End}(E)$ is a quadratic imaginary order of discriminant prime to p, and p splits into $\mathfrak{p}_1\mathfrak{p}_2$, one ideal corresponding to the Frobenius and the other to the Verschiebung. If $E/\mathbb{F}_q$ is supersingular, then $\operatorname{End}(E)$ is a maximal order $\mathcal{O}$ in a quaternion algebra ramified at p and infinity $B_{p,\infty}$. The completion $\mathcal{O}$ is the unique valuation ring in $B_{p,\infty} \otimes \mathbb{Q}_p$. If R is a primitive orientation, then R is locally maximal at p, and p is either inert or ramified. □

If $E/\mathbb{F}_q$ is ordinary, or if $E/\mathbb{F}_p$ is supersingular defined over $k = \mathbb{F}_p$, then if E is primitively R-oriented we have $R = \operatorname{End}_k(E)$, because $\operatorname{End}_k(E)$ is of rank 2. In both cases the orientation is given by the Frobenius endomorphism π_k, and every isogeny respecting the orientations [Aurel : Tu n'as pas justement défini "R-oriented" pour abbrévier "respecting the orientation" ?] is a rational isogeny. In these two cases, the functor $\mathcal{HOM}_R(\cdot,E)$ is an equivalence of category:

Theorem 2.7. *Let $E/\mathbb{F}_q$ be an elliptic curve with a primitive orientation by an imaginary quadratic order R. Assume that either E is ordinary or E is supersingular and that $q = p$. Then $\mathcal{HOM}_R(\cdot,E)$ is an equivalence of categories between torsion free f.p. R-modules and R-oriented abelian varieties isogenous to E^n with isogenies respecting the orientation.*

Proof. Let $f_R = f_E$ be the conductor of $R = \mathrm{End}_k(E)$. By [JKP+18, Theorem 7.5 and Theorem 7.11], $\mathcal{HOM}_R(\cdot, E)$ is an equivalence of categories between torsion free f.p. R-modules and abelian varieties A isogenous to E^n with conductor $f_A \mid f_E$. Such abelian varieties split as a product $A = E_1 \times \cdots \times E_n$, and $f_A \mid f_E$ is equivalent to $f_{E_i} \mid f_E$ for all i.

In particular, $R \subset \mathrm{End}_k(E_i)$ for all i, and the diagonal action gives a natural orientation on A, which is induced by the Frobenius endomorphism. The isogeny $E^n \to A$ is rational and therefore respects this orientation.

Conversely, if $\phi\colon E^n \to A$ is an R-oriented rational isogeny, then the first paragraph in the proof of [JKP+18, Theorem 6.5] shows that A is in the image of $\mathcal{HOM}_R(\cdot, E)$. □

It remains to treat the case of a supersingular curve $E/\mathbb{F}_{p^2}$ with rank 4 endomorphism ring. In this case, the functor $\mathcal{HOM}_R(\cdot, E)$ gives an embedding from torsion free f.p. R-modules to oriented abelian varieties isogenous to E^n, but it is not necessarily surjective.

Theorem 2.8. *Let $E/\mathbb{F}_q$ be an elliptic curve with a primitive orientation by an imaginary quadratic order R. Then the functor $\mathcal{HOM}_R(\cdot, E)$ is fully faithful and admits as an inverse on its image the functor $\mathrm{Hom}_R(\cdot, E)$ that sends R-oriented abelian variety A to the module of R-oriented isogenies.*

Proof. By the same proof as in [JKP+18, Theorem 4.8], this reduces to proving that

$$\mathrm{Hom}_R(\mathfrak{b}, \mathfrak{a}) \simeq \mathrm{Hom}_R(\mathcal{HOM}_R(\mathfrak{a}, E), \mathcal{HOM}_R(\mathfrak{b}, E))$$

for two ideals $\mathfrak{a}, \mathfrak{b}$ of R. The non oriented case follows from [Kan11, Proposition 10 and Proposition 17], which we need to adapt to the oriented case.

Let K_1, K_2 be two subgroup schemes of E stable by R such that E/K_1 is R-isomorphic to E/K_2. Then the proof of [Wat69, p. 532] shows that there exists an element $\gamma \in \mathrm{End}^0(E)$ in the centralizer R' of R in $\mathrm{End}(E/K_1)$, and an $n \in \mathbb{Z}$ such that $\gamma^{-1}(K_1) = [n]^{-1}(K_2)$. Since R is of rank 2, this centralizer is the saturation of R in $\mathrm{End}(E/K_1)$. (By assumption, R is a primitive orientation of E but may not be saturated in $\mathrm{End}(E/K_1)$.) So modifying n if necessary we may assume that $\gamma \in R$. This extends [Kan11, Equation 17] to the oriented case, and the rest of the proof of [Kan11, Proposition 10] applies. □

As mentioned above, there is an obstruction to being in the essential image of $\mathcal{HOM}_R(\cdot, E)$. We need to identify R-oriented abelian varieties A isogenous to E^n that belong to the image of $\mathcal{HOM}_R(\cdot, E)$. If $\phi\colon E^n \to A$ is an R-isogeny, its kernel K is stable by R, and by [JKP+18, Proposition 6.3] the question is whether K can be built as the kernel of an R-morphism $E^n \to E^m$. Note that by fully faithfulness (see Theorem 2.8), the answer does not depend on the isogeny ϕ [Aurel : Tu veux dire que ça dépend seulement de A?].

Given an R-oriented abelian variety A, we let ρ_A be the $\mathbb{F}_p$-representation of R/pR on $\mathrm{Lie}(A)$ given by the action on differentials. If $\phi\colon A \to B$ is an oriented morphism induced by $\mathcal{HOM}_R(\cdot, E)$ from a module morphism $\psi\colon M_B \to M_A$, then by Theorem 2.4 applied to $k' = k[\epsilon]/(\epsilon^2)$, ϕ induces a morphism of representations between ρ_A and ρ_B. We will show that if A is induced by a torsion free module of rank n, then ρ_A has to be equivalent to ρ_E^n, and that this is the only obstruction.

Theorem 2.9. *Let E be an elliptic curve with a primitive orientation by an imaginary quadratic order R. If E is supersingular, we assume furthermore that E is defined over $\mathbb{F}_p$ or that it is defined over $\mathbb{F}_{p^2}$ with full endomorphism ring.*

Then the fully faithful exact functor $\mathcal{HOM}_R(\cdot, E)$ between torsion free f.p. R-modules and R-oriented abelian varieties isogenous to E^n with isogenies respecting the orientation has essential image consisting of the abelian varieties A that are R-isogenous to E^n and such that $\rho_A \simeq \rho_E^n$. In particular we have an equivalence of categories whenever p is split in R (which is equivalent to E being ordinary) or ramified.

Proof. Theorem 2.7 already handles the case of E ordinary or E supersingular defined over $\mathbb{F}_p$. In both cases, p is either split ($p = \mathfrak{p}\bar{\mathfrak{p}}$) or ramified ($p = \mathfrak{p}^2$), with $\rho(\mathfrak{p}) = 0$: since the Frobenius is purely inseparable, it acts trivially on the tangent space. Hence the representation ρ_A descends to a $\mathbb{F}_p$-representation of $\mathbb{F}_p$, so is automatically compatible.

It remains to handle the case of E supersingular defined over $\mathbb{F}_{p^2}$. The same argument as in [JKP+18, § 6.3] shows that a prime-to-p oriented subgroup comes from a module map. Indeed, if ℓ is prime to p,

the centralizer C_ℓ of R_ℓ in $\mathrm{End}(T_\ell E)$ is R_ℓ itself by [JKP+18, (ii) p.16], and if $K \subset E[\ell^e]$ is an R-stable subgroup scheme, $K(k_s)$ is a $C_\ell/\ell^e C_\ell$-submodule of E, and we apply the same proof as in [JKP+18, Proposition 6.8].

So the only obstruction must come from inseparable isogenies. We first look at the case of dimension 1. Every isogeny is the composition of a separable isogeny with some power of the Frobenius. Since $\pi_p^2 = [p]$, we need to check whether $\pi_p \colon E \to E^{(p)}$ is induced by an ideal. Its kernel α_p is stable by R since α_p is the unique subgroup of index p of $E[p]$. If $p = \mathfrak{p}^2$ is ramified in R, then π_p is induced by $\mathfrak{p}$, but if p is inert, then π_p cannot induced by an ideal since there are no ideals of norm p in R. Thus in that case there are two components in dimension 1: any R-isogeny from E comes from a separable isogeny from either E or its Galois conjugate $E^{(p)}$. Furthermore, ρ_E is a representation of $R/pR \simeq \mathbb{F}_{p^2}$ on $\mathrm{Lie}\, E$, and $\rho_{E^{(p)}}$ is its Galois conjugate, which is not equivalent to the first representation. So we can use ρ to check on which of the two components we are.

In higher dimension, by the Chinese Remainder Theorem, every oriented isogeny $\phi \colon E^n \to A$ decomposes as an inseparable oriented isogeny $\phi' \colon E^n \to A'$, and an oriented isogeny with prime to p kernel $\phi'' \colon A' \to A$. Moreover, every inseparable isogeny is a composition of isogenies with kernel α_p by [JKP+18, Lemma 5.9]. If the isogeny ϕ' is oriented, then since R is commutative of discriminant prime to p, its action on the p-torsion is semisimple so we may always find an α_p that is stable by R.

The group $\mathrm{Gl}_n(R)$ acts transitively on the non zero elements of $\mathrm{Hom}_R(\alpha_p, E^n) \simeq \mathbb{F}_{\mathfrak{p}}^n$ (where the action of R on α_p is then one induced by the inclusion $\alpha_p \subset E[p]$ and $\mathfrak{p}$ is the prime ideal of R above p). So we may assume that α_p is contained in $E \times 0 \times \cdots \times 0$, and that the isogenous curve is isomorphic to $E^{(p)} \times E \cdots \times E$. By recurrence, assume that the domain is ${E^{(p)}}^{m_1} \times E^{m_2}$. By looking at the Dieudonné modules, we see that there are two possible action of R on our kernel α_p, and depending on the action, either α_p has no R-embedding to E^{m_2} or no R-embedding to ${E^{(p)}}^{m_1}$. We then use the action of $\mathrm{Gl}_{m_1}(R)$ on ${E^{(p)}}^{m_1}$ (via its twisted action on $E^{(p)}$) or of $\mathrm{Gl}_{m_2}(R)$ on E^{m_2} to see that the quotient is still isomorphic to ${E^{(p)}}^{m_1'} \times E^{m_2'}$.

Now, if $A' = {E^{(p)}}^{m_1} \times E^{m_2}$ with its natural product R-orientation, then $\rho_{A'} \simeq \overline{\rho_E}^{m_1} \oplus \rho_E^{m_2}$. Furthermore, the separable isogeny $\phi'' \colon A' \to A$ induces an equivalence of representation $\rho_{A'} \simeq \rho_A$. In particular, if $\rho_A \simeq \rho_E^n$, then A' has to be isomorphic to E^n. Since the isogeny $\phi'' \colon E^n \to A$ is represented by a module map, we see that A is in the image of $\mathcal{HOM}_R(\cdot, E)$.

We remark that, since by [Oda69, Corollary 5.11], the Dieudonné module of $A[p]$ of an abelian variety is canonically isomorphic to its first De Rham cohomology, and the Frobenius filtration on $A[p]$ corresponds via the Dieudonné functor, to the Hodge filtration (up to a Galois twist), its it not surprising that we can read off on the differentials of A the information about the inseparable part of the isogeny $E^m \to A$.

Conversely, if $A = \mathcal{HOM}_R(M, E)$, then by Lemma 2.5, the module M is isomorphic to a sum of ideals $M = \oplus \mathfrak{a}_i$, so A is isomorphic to a product of elliptic curves $A = \prod E_i$, with each E_i being R-oriented and A given the natural product orientation. Furthermore, since the conductor of R is not divisible by p, we can assume that the $\mathfrak{a}_i$ have norm coprime to p, so that the ideals $\mathfrak{a}_i$ give a separable oriented isogeny $E \to E_i$, in particular $\rho_E \simeq \rho_{E_i}$, hence $\rho_A \simeq \rho_E^n$.

□

Remark 2.10.

- In dimension 1, restricting to invertible ideals, we recover the oriented group action of [CK20; Onu21]. However our equivalence handles the case of non invertible ideals (which go up in the oriented volcano), and does not rely on a CM lift to characteristic zero.
- If $E/\mathbb{F}_{p^2}$ is a supersingular curve with endomorphism ring $\mathcal{O}$ of rank 4, in [JKP+18, Theorem 5.3], the authors prove an equivalence of categories $\mathcal{HOM}_{\mathcal{O}}(\cdot, E)$ between abelian varieties and torsion free f.p. $\mathcal{O}$-modules.

  We note that, restricting to rank 1 modules, this corresponds to the original version of Deuring's correspondence, between left $\mathcal{O}$-ideals and supersingular curves E' isogenous to E. The only difference is that Deuring's version uses an equivalence, and the inverse map is given

by $\mathrm{Hom}(E, E')$ which is a left $\mathcal{O}$-ideal, while we use a contravariant version and the inverse map is given by $\mathrm{Hom}(E', E)$, which is a right $\mathcal{O}$-ideal.

The Deuring correspondence is often described in terms of maximal orders (a maximal order giving a supersingular curve), and isogenies described in term of ideals. The link with the previous description is that with a left $\mathcal{O}$-ideal we associate its right order $\mathcal{O}'$, and with an order $\mathcal{O}'$ we associate a connecting $(\mathcal{O}, \mathcal{O}')$-ideal. For more details we refer to [Voi21; Ler22].

Now, if $R \subset \mathcal{O}$ is a primitive embedding, by the construction of $\mathcal{HOM}_R(\cdot, E)$ and $\mathcal{HOM}_{\mathcal{O}}(\cdot, E)$, if M is a torsion free R-module, then $\mathcal{HOM}_R(M, E) = \mathcal{HOM}_{\mathcal{O}}(M \otimes_R \mathcal{O}, E)$.

We remark that $M \otimes_R \mathcal{O}$ has a natural structure of $(R, \mathcal{O})$-bimodule, and via the equivalence of categories $\mathcal{HOM}_R(\cdot, E)$, an oriented isogeny between $\mathcal{HOM}_{\mathcal{O}}(M_1 \otimes_R \mathcal{O}, E)$ and $\mathcal{HOM}_{\mathcal{O}}(M_2 \otimes_R \mathcal{O}, E)$ corresponds to a R-module morphism $M_2 \otimes_R \mathcal{O} \to M_1 \otimes_R \mathcal{O}$ that is also a morphism of $(R, \mathcal{O})$-bimodules. Since R is its own centralizer in $\mathcal{O}$, such a morphism descends to a morphism of R-modules $M_2 \to M_1$. This gives an alternative proof of Theorem 2.8.

The functor $M \mapsto M \otimes_R \mathcal{O}$ gives a way to study the forgetting of orientation functor (as done in [ACL+22]) purely at the module level.

Now that we have our equivalence, we want to restrict it to principally polarised abelian varieties and N-isogenies. If M is a torsion free f.p. left R-module, then the dual $M^* = \mathrm{Hom}_R(M, R)$ has a natural structure of right R-module. Using the Rosati involution $x \mapsto \overline{x}$, M^* becomes a left R-module: the module of R-antilinear maps $M \to R$. [Aurel : Ce paragraphe n'est pas très clair. On a l'impression que tu changes la définition de M^*. Je pense qu'il faut que tu écrives explicitement quelle est ta structure de R-module de M^* parce qu'à première vue il y en a plusieurs possibles.] A map $\psi\colon M \to M^*$ is said to be symmetric if $\psi^*\colon M^{**} = M \to M^*$ is equal to ψ. Given such a symmetric ψ, we can define a Hermitian form H_ψ by $H_\psi(m_1, m_2) = \psi(m_2)(m_1)$ (see Section 4 for more details on Hermitian forms). Conversely, a Hermitian form H on M induces a symmetric map $M \to M^*$. We say that H is an integral Hermitian form on M, and that (M, H) is unimodular if H induces an isomorphism $M \simeq M^*$.

Theorem 2.11. *Under the functor above $\mathcal{HOM}_R(\cdot, E)$, a polarisation on $A = \mathcal{HOM}_R(M, E)$ corresponds to an integral positive definite Hermitian form H on M^*, a principally polarisation to a unimodular Hermitian form on M^* (equivalently an unimodular Hermitian form H_M on M), and a N-isogeny $f\colon A \to B$ of ppavs to a similitude of multiplier N with respect to the Hermitian forms: $\phi\colon (M_B, H_B) \to (M_A, H_A)$ satisfy $\phi^* H_A = N H_B$.*

Proof. We recall that a polarisation $A \to A^\vee$ is a morphism $A \to A^\vee$ that is symmetric (i.e., self-dual), and is induced by an ample line bundle. We need to translate these conditions on the module side, via our equivalence of categories.

The same proof as in [JKP+18, § 4.3] shows that if $A = \mathcal{HOM}_R(M, E)$, then $A^\vee = \mathcal{HOM}_R(M^*, E)$, where M^* is the R-dual of M, with R acting on the right on M^*, or on the left via the Rosatti involution. Via our orientation, the Rosatti involution is given by $\bar{\cdot}$ on R. The dual of the isogeny associated with $N \to M$ corresponds to the dual map $M^* \to N^*$. Finally, we have the biduality $M \simeq M^{**}$ given by $m \mapsto (\psi \mapsto \overline{\psi(m)})$.

By biduality, a symmetric isogeny $f\colon A \to A^\vee$ thus correspond to a Hermitian form H on M^*, interpreted as a morphism $M^* \to M$ (with the R-module structure on M^* given by the Rosatt involution as mentioned above).

By [KNRR21, Theorem 3.3], this symmetric isogeny comes from an ample line bundle precisely when the Hermitian form is positive definite. We sketch the argument: A is isogenous to E^g, there is a map $E^g \to A$ which is finite faithfully flat, so by descent we reduce to the case $A = E^g$. Now on E^g we have the canonical product polarisation, while on the Hermitian side we have the canonical positive definite Hermitian form $(R^n, H_R \oplus \cdots \oplus H_R)$. The other polarisations (resp. positive definite Hermitian forms) are given by the action of totally positive endomorphisms on E^g in both cases, and it follows that ampleness is equivalent to the positive definite condition.

If $f\colon A \to B$ is an isogeny corresponding to the linear map $\phi\colon N \to M$, and we have principal polarisations ϕ_A, ϕ_B on A, B associated with Hermitian forms H_A, H_B, then the contragredient isogeny $\tilde{f}\colon B \to A = \phi_A^{-1} \circ \hat{f} \circ \phi_B$ corresponds to the dual ϕ^* of ϕ with respect to the Hermitian forms. By

definition, f is an N-isogeny if and only if $f \circ \tilde{f} = \tilde{f} \circ f = N$, if and only if ϕ is a N-similitude, if and only if $\phi^* H_A = N H_B$. □

Remark 2.12. If (M, H) is a torsion free Hermitian R-module, the Hermitian form extends to $V = M \otimes \mathbb{Q}$. Conversely, if (V, H) is a Hermitian $R \otimes \mathbb{Q}$ vector space, and M a R-sublattice, then H induces an isomorphism $V \to V^*$ and an isomorphism $M^\sharp \to M^*$ where $M^\sharp = \{m' \in V, H(m', M) \subset R\}$. The module M^* is integral if and only if $M^\sharp \subset M$. In this case, the corresponding polarisation on $A = \mathcal{HOM}_R(M, E)$ has kernel $\mathcal{HOM}_R(M/M^\sharp, E)$, so is of degree the cardinal of $M/M^\sharp$ by Theorem 2.4. We refer to [KNRR21, § 3.1] for more details.

Corollary 2.13. *Let A be a principally polarised abelian variety corresponding to the unimodular Hermitian module (M_A, H_A). Then kernels $\operatorname{Ker}\phi$ of N-isogenies $\phi\colon A \to B$ correspond bijectively to submodules $M_B \subset M_A$ such that $M_B^\sharp := \{m \in M_A \otimes \mathbb{Q}, H_A(m, M_B) \subset R\} = \frac{1}{N} M_B$.*

Proof. By exactness of $\mathcal{HOM}_R(\cdot, E)$, since an isogeny is an epimorphism between abelian varieties of the same dimension, it corresponds to a monomorphism between torsion free modules $M_B \subset M_A$ of the same rank. By Theorem 2.11, ϕ is an N-isogeny if and only if M_B is unimodular for $H_B = \frac{1}{N} H_A$ if and only if the orthogonal of M_B for H_A is exactly $\frac{1}{N} M_B$ (in which case the rank condition is automatic). □

Example 2.14. Let $\mathfrak{a}$ be an ideal in R. By Theorem 2.4, the map $\mathfrak{a} \to R$ corresponds to the isogeny $\phi_\mathfrak{a}\colon E \to E_\mathfrak{a}$. By Definition 2.3, if $\mathfrak{a} = R\mathcal{N}(\mathfrak{a}) + R\mu$, these two generators give a surjection $R^2 \twoheadrightarrow \mathfrak{a} \subset R$ hence corresponds to an embedding $i_\mathfrak{a}\colon E_\mathfrak{a} \to E^2$. The map $E \to E^2$, $\phi\colon (P, Q) \mapsto (\mathcal{N}(\mathfrak{a})P, \mu Q)$, whose kernel is $E[\mathcal{N}(\mathfrak{a}), \mu] = E[\mathfrak{a}]$, factorize through this embedding. We will revisit this in Section 3.1 for the case of a general module.

The principal polarisation on E corresponds to the canonical Hermitian form on R: $H_R(x, x) = x\overline{x} = \mathcal{N}(x)$. Since f [Aurel : Je suis perdu, c'est qui f? $\phi_\mathfrak{a}$?] is an $\mathcal{N}(\mathfrak{a})$-isogeny, it follows that the principal polarisation on $E_\mathfrak{a}$ is given by $H_R/\mathcal{N}(\mathfrak{a})$. This can also be seen from the fact that since $\mathfrak{a}\overline{\mathfrak{a}} = \mathcal{N}(\mathfrak{a})$, then for H_R, the orthogonal of $\mathfrak{a}$ is given by $\mathfrak{a}/\mathcal{N}(\mathfrak{a})$.

Let $\gamma \in R \otimes \mathbb{Q}$ be such that $\mathfrak{b} = \gamma\mathfrak{a} \subset R$ is an integral ideal. We have $\mathcal{N}(\gamma) = \mathcal{N}(\mathfrak{b})/\mathcal{N}(\mathfrak{a})$. The map $\gamma\colon (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \to (R, H_R), x \mapsto \gamma x$ is a $\mathcal{N}(\mathfrak{a})\gamma\overline{\gamma} = \mathcal{N}(\mathfrak{b})$-similitude. A way to find such a γ is to sample a $\gamma' \in \mathfrak{a}$, and take $\gamma = \overline{\gamma'}/\mathcal{N}(\mathfrak{a})$. If $\mathcal{N}(\gamma') = r\,\mathcal{N}(\mathfrak{a})$, we then have $\mathcal{N}(\mathfrak{b}) = r$.

Alternatively, the map $\mathfrak{b} \to R$ induces a $\mathcal{N}(\mathfrak{b})$-isogeny $E \to E_\mathfrak{b}$, and $\gamma\colon (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \to (\mathfrak{b}, H_R/\mathcal{N}(\mathfrak{b}))$ induces an isomorphism $E_\mathfrak{b} \to E_\mathfrak{a}$ since γ is an 1-similitude.

The element $\gamma' \in \mathfrak{a}$ gives an endomorphism of R which factorize as a map $(R, H_R) \to (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \to (R, H_R)$, which corresponds to a map $E \to E_\mathfrak{a} \to E$, with $\phi_\mathfrak{a}\colon E \to E_\mathfrak{a}$ the canonical $\mathcal{N}(\mathfrak{a})$-isogeny associated with $\mathfrak{a}$ and $\phi_{\gamma'}\colon E_\mathfrak{a} \to E$ a $\mathcal{N}(\gamma')/\mathcal{N}(\mathfrak{a})$-isogeny. Taking duals, we get that the adjoint of $\gamma\colon (R, H_R) \to (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a}))$ is $\gamma = \overline{\gamma'}/\mathcal{N}(\mathfrak{a})\colon (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \to (R, H_R)$ giving the dual isogeny $\tilde{\phi_{\gamma'}}\colon E \to E_\mathfrak{a}$, which corresponds exactly to $\phi_\mathfrak{b}$ where $\mathfrak{b} = \gamma\mathfrak{a}$ as above. And in fact, given the presentation $R^2 \to \mathfrak{a}$ given by the two generators $(\mathcal{N}(\mathfrak{a}), \mu)$ as above, composing this map with $\overline{\gamma'}/\mathcal{N}(\mathfrak{a})$ we get a presentation $R^2 \twoheadrightarrow \mathfrak{b} = (\mathcal{N}(\mathfrak{b}), \mu\overline{\gamma'}/\mathcal{N}(\mathfrak{a}))$. Composing further with the canonical inclusion $\mathfrak{b} \subset R$, we get the map $E \to E^2, (P, Q) \mapsto (\mathcal{N}(\mathfrak{b})P, \mu\overline{\gamma'}/\mathcal{N}(\mathfrak{a}))$ whose kernel is precisely $E[\mathfrak{b}]$, hence whose image is $E_\mathfrak{b}$. So our equivalence of categories $\mathcal{HOM}_R(\cdot, E)$ behaves as expected on ideals, and in particular correctly associates with $\gamma' \in \mathfrak{a}$ the $\mathcal{N}(\gamma')/\mathcal{N}(\mathfrak{a})$-isogeny $E \to E_\mathfrak{a}$ associated with $\mathfrak{b} = \gamma'\mathfrak{a}$.

The adjoint of the inclusion $(\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \to (R, H_R)$ is $[\mathcal{N}(\mathfrak{a})]\colon (R, H_R) \to (\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a}))$ corresponding to the isogeny $\tilde{\phi_\mathfrak{a}}\colon E_\mathfrak{a} \to E$ which factorizes through $[\mathcal{N}(\mathfrak{a})]\colon E \to E$, and the composition $[\mathcal{N}(\mathfrak{a})] \circ \tilde{\phi_{\gamma'}}\colon E \to E_\mathfrak{a} \to E$ gives the dual endomorphism $\overline{\gamma'}$ of γ' as expected.

3. Translating between modules and abelian varieties

In this section we explain how to translate a module map into an oriented isogeny. Again for our application to the class group action, we only need a very special case, but since it may be useful in other context, we treat the general case here.

Most of the problems in the Deuring correspondence have a similar version in our setting. We only sketch them briefly in this section, and raise some open questions along the way.

Let $E/\mathbb{F}_q$ be an R-oriented elliptic curve, with the orientation effective. This means that we should be able to evaluate the action of some endomorphism $\gamma \in R \setminus \mathbb{Z}$ in polynomial time (in the discriminant of R and $\log q$). Every other endomorphism is of the form $a/f + b/f \cdot \gamma$, and we can use the division algorithm of [Rob22b] to evaluate it efficiently. (We will only need to compute the action of endomorphisms in R on points defined over $\mathbb{F}_q$ or a small field extension, so we can always reduce our integers modulo $\#E(\mathbb{F}_q)$ to reduce the height of our endomorphisms).

In particular, if $E/\mathbb{F}_q$ is ordinary or a supersingular curve defined over $\mathbb{F}_p$, then the Frobenius π_q is an efficient endomorphism, and since the orientation is induced by π_q it is always effective. However, if $E/\mathbb{F}_q$ is a supersingular curve defined over $\mathbb{F}_{q^2}$, we do need an efficient representation of our orientation (such an efficient representation always exists by [Rob22a]). Such an efficient representation can be found if $\mathrm{End}(E)$ is known.

3.1. **Presentations of abelian varieties.**

Definition 3.1. Let M be a torsion free f.p. R-module, and let $R^m \to R^n \twoheadrightarrow M$ be a presentation of M. By Section 2, the abelian variety $A = \mathcal{HOM}_R(M, E)$ is the kernel of the matrix (acting on the right) $X \colon E^n \to E^m$ associated with this presentation.

An effective (full) presentation of A is a given explicit model of A, along with an efficient way to compute the embedding $i_A \colon A \hookrightarrow E^n \to E^m$. We will often only need the first map $i_A \colon A \hookrightarrow E^n$ which we still call a (partial) presentation.

Technically, we should consider i_A as a copresentation, but we will use the term presentation for the sake of simplicity. Notice that since A is the kernel of an explicit matrix of endomorphisms $E^n \to E^m$, we always have an implicit description of the torsion points $A[\ell]$ as the kernel of the induced map $E^n[\ell] \to E^m[\ell]$. Having an efficient representation is a way to map between a concrete model of A and the implicit model as the kernel of $E^n \to E^m$.

Lemma 3.2. *If $A = \mathcal{HOM}_R(M, E)$ and $i_A \colon A \hookrightarrow E^n \to E^m$ is an effective presentation of A, then any other presentation $X' \colon R^{m'} \to R^{n'} \twoheadrightarrow M$ gives an effective presentation $i'_A \colon A \hookrightarrow E^{n'} \to E^{m'}$ of A.*

Proof. The map $R^{n'} \twoheadrightarrow M$ factorizes through $R^n \twoheadrightarrow M$, hence $i'_A \colon A \hookrightarrow E^{n'}$ factorizes as $A \to E^n \to E^{n'}$, where $i_A \colon A \to E^n$ is effective by hypothesis, and $E^n \to E^{n'}$ is given by a matrix of endomorphisms. □

Example 3.3. We revisit Example 2.14. Let $\mathfrak{a} \subset R$ be an ideal, we can always find an element $\mu \in \mathfrak{a}$ such that $\mathfrak{a} = (\mathcal{N}(\mathfrak{a}), \mu)$. We have a presentation $R^m \to R^2 \twoheadrightarrow \mathfrak{a}$, where the map on the right is $(x, y) \mapsto x\mathcal{N}(\mathfrak{a}) + y\mu$. Let $E_\mathfrak{a} = E/E[\mathfrak{a}]$ be the elliptic curve corresponding to $\mathfrak{a}$, the map $R^2 \to \mathfrak{a} \subset R$ induces $E \to E_\mathfrak{a} \to E^2$ whose composition $\phi \colon (P, Q) \mapsto (\mathcal{N}(\mathfrak{a})P, \mu Q)$ factorizes through the embedding $i_\mathfrak{a} \colon E_\mathfrak{a} \to E^2$. And the image of ϕ, whose kernel is $E[\mathcal{N}(\mathfrak{a}), \mu]$, is precisely $E_\mathfrak{a}$.

This gives an explicit embedding of $E_\mathfrak{a}$ into E^2 which we call a presentation, we can thus work on torsion points of $E_\mathfrak{a}$ abstractly. However in general the resulting image curve will be of very high degree, so it seems hard to directly recover a Weierstrass equation for $E_\mathfrak{a}$ (e.g. by interpolation). In Section 5, we will give another approach to compute $E_\mathfrak{a}$.

Example 3.4. It is customary in effective versions of the Deuring correspondence to construct two paths $\phi_1 \colon E \to E_0$, $\phi_2 \colon E \to E_0$ of coprime degrees, where E_0 is some special nice supersingular curve. The map $(\phi_1, \phi_2) \colon E \to E_0^2$ can be seen as a presentation of E for the equivalence of categories $\mathcal{HOM}_{\mathrm{End}(E_0)}(\cdot, E_0)$ of Remark 2.10.

Let $\psi \colon M_2 \to M_1$ be a map of torsion free f.p. R-modules, and $\phi \colon A_1 \to A_2$ the corresponding morphism of oriented abelian varieties. When ϕ is an N-isogeny (so M_1, M_2 are unimodular Hermitian modules and ψ an N-similitude), then given an effective presentation of A_1, we will use the same techniques as in [KNRR21, § 3.3] to compute ϕ.

Lemma 3.5. *Let $\psi \colon M_2 \to M_1$ be a map of torsion free f.p. R-modules, and $\phi \colon A_1 \to A_2$ the corresponding morphism of oriented abelian varieties. Given presentations $i_{A_1} \colon A_1 \hookrightarrow E^{n_1}$ of A_1, and*

$i_{A_2}\colon A_2 \hookrightarrow E^{n_2}$ of A_2, the map $i_{A_2}\circ\phi$ factorize through a map $\tilde{\phi}\colon E^{n_1}\to E^{n_2}$:

$$\begin{array}{ccc} A_1 & \xrightarrow{i_{A_1}} & E^{n_1} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \tilde{\phi}} \\ A_2 & \xrightarrow{i_{A_2}} & E^{n_2} \end{array}$$

We say that $\tilde{\phi}$ is a presentation of ϕ.

Proof. The presentation $A_1 \hookrightarrow E^{n_1}$ is induced by a surjective map $R^{n_1} \twoheadrightarrow M_1$, and $A_2 \hookrightarrow E^{n_2}$ by a surjective map $R^{n_2} \twoheadrightarrow M_2$. Since the module R^{n_2} is projective, the map $R^{n_2} \twoheadrightarrow M_2 \to M_1$ factorize as a map $R^{n_2} \to R^{n_1} \to M_1$. □

Note that $\operatorname{Ker}\phi = \operatorname{Ker}\tilde{\phi} \cap i_{A_1}(A_1)$. Since $\tilde{\phi}$ is given by a matrix of endomorphisms and the orientation is effective, we can compute its kernel; so if we have an effective presentation of A_1 we can compute the kernel of ϕ.

3.2. **Submodules, kernels, and isogenies.** Let $A = \mathcal{HOM}_R(M, E)$ be an abelian variety represented by the module M. An element $m \in M$ corresponds to a morphism $R \to M\colon r \mapsto r\cdot m$, hence to a morphism $\phi_m\colon A \to E$. We can thus interpret m as a "function map" on A via ϕ_m, and we denote by $A[m]$ the kernel of ϕ_m.

Lemma 3.6. *Let $M' \subset M$ be a submodule of M, let $A = \mathcal{HOM}_R(M, E)$ and $B = \mathcal{HOM}_R(M', E)$. The surjective morphism $\phi\colon A \to B$ corresponding to the inclusion $M' \to M$ has kernel $\operatorname{Ker}\phi \simeq \mathcal{HOM}_R(M/M', E) \simeq A[M'] \coloneqq \cap A[m_i]$ for any generating set $(m_1, \dots, m_r)$ of M'.*

Proof. By exactness, the kernel of ϕ corresponds to the cokernel M/M'. The generators m_i induce a presentation $R^r \twoheadrightarrow M'$ which, composed with the inclusion, yields a map $\psi\colon R^r \to M$ whose cokernel is isomorphic to M/M'. On the abelian variety side, the presentation of M' gives an embedding $i_B\colon B \to E^r$ as in Section 3.1, and the kernel of ϕ is the kernel of $i_B \circ \phi$. A point $P \in A$ is in this kernel if and only if $\pi_i(i_B \circ \phi(P)) = 0_E$ for all projections $\pi_i\colon E^r \to E$, but by construction $\pi_i \circ i_b \circ \phi$ is the map corresponding to the module element m_i. Hence $\operatorname{Ker}\phi = \cap A[m_i]$. □

Conversely, given a subgroup K of A, we can let $M_K \subset M$ be the submodule $\{m \in M, K \subset A[m]\}$. By definition, we have $K \subset A[M_K]$.

Lemma 3.7. *With the notations above, $K = A[M']$ for some submodule $M' \subset M$ if and only if $B \coloneqq A/K$ is represented by a module M_B. In this case, $M' = M_K \simeq M_B$ and $B \simeq \mathcal{HOM}_R(M_K, E)$, $K \simeq \mathcal{HOM}_R(M/M_K, E)$.*

Proof. This follows immediately from our equivalence of categories from Section 2. [Aurel : peut-être citer le thm précis ici ?] □

Corollary 3.8. *Let $K \subset A$ be a finite subgroup scheme stable by R. Assume that either p is not inert in R, or that K is étale. Then $K = A[M_K]$.*

Proof. If $B = A/K$, then the R-orientation on A descends to B, and B is R-isogenous to E^g since A is. By Theorem 2.9, under our assumptions B is induced by a module, so we can apply Lemma 3.7. □

Example 3.9. Let $\psi\colon M_1 \to M_2$ be a map of R-modules, it factorizes as $M_1 \twoheadrightarrow M_2' \hookrightarrow M_2$, and the corresponding map of abelian varieties $\phi\colon A_2 \to A_1$ factorizes as $A_2 \twoheadrightarrow A_2' \hookrightarrow A_1$. The kernel of $A_2 \twoheadrightarrow A_2'$ is given by $A_2[M_2']$.

Example 3.10. By Theorem 2.11, an isogeny $\phi\colon A \to \hat{A}$ corresponds to a Hermitian form H_V on $V = M \otimes \mathbb{Q}$, along with an inclusion $M^\sharp \subset M$. In this case H_V induces an isomorphism $M^* \simeq M^\sharp$, and we have $\operatorname{Ker}\phi = A[M^\sharp]$.

A presentation $i_A\colon A \to E^n$ induced by $R^n \twoheadrightarrow M$ induces by duality a surjection $E^n \twoheadrightarrow \hat{A}$ via $M^* \hookrightarrow R^n$.

Example 3.11. Let (M, H_M) be a unimodular Hermitian R-module, $V = M \otimes \mathbb{Q}$. Since $M^\sharp = M$, a submodule $M' \subset M$ satisfies $M' \subset M \subset M'^\sharp$, since the restriction of H_M to M' is still integral. By Corollary 2.13, the inclusion $M' \subset M$ corresponds to a N-similitude, with $H_{M'} = \frac{1}{N} H_M$, if and only if $M'^\sharp = \frac{1}{N} M'$.

Given an explicit presentation $i_A \colon A \to E^n$ of A, corresponding to generators $m_1, \dots, m_n$ of M, then any element m can be written $m = \sum r_i m_i$. Since the presentation i_A is effective and the orientation by R on E is effective too, we can compute the action of m on the N-torsion on A. This gives a way to compute the kernel associated with an isogeny of exponent N (in particular associated with an N-similitude) whenever N is smooth and the N-torsion of E is accessible.

Conversely, if we have an isogeny $\phi \colon A \to B$ that we know is represented by a module map $M' \subset M$ and $\operatorname{Ker} \phi \subset A[N]$, we can find M' by looking at the action of the m_i on $A[N]$ and solving some DLPs. If $m' \in M'$, and we want to evaluate m' on some point $Q \in B$, by construction we have $m'(Q) = m'(P)$ for any $P \in \phi^{-1}(Q)$. Indeed, since $m' \in M'$, $\operatorname{Ker} m' \supset \operatorname{Ker} \phi$ so m' factorizes through B. Finding P however might be difficult if ϕ has large degree, and we will come back to this question in Section 3.3.

3.3. **Smooth similitude to isogeny.** Let $\psi \colon (M_1, H_1) \to (M_2, H_2)$ be an N-similitude of unimodular Hermitian R-modules, $\phi \colon A_2 \to A_1$ the corresponding N-isogeny of ppavs. Taking a presentation $\tilde{\psi}$ of ψ as in Lemma 3.5; we recover the kernel of ϕ, alternatively we have $\operatorname{Ker} \phi = A[\psi(M_1)]$. Since we can compute the kernel of ϕ, we can use an isogeny algorithm (such as [LR22]) to compute it. The complexity of this computation will depend on the smoothness bound on N and whether the N-torsion is accessible.

Now if we want to iterate our construction (typically to split a large isogeny into several blocks), we also need a way to describe the presentation $i_{A_2} \colon A_2 \to E^{n_2}$ (or any other presentation by Lemma 3.2).

We note that our construction above gives the value of i_{A_2} on $\phi(P)$ for $P \in A_1$; however given $Q \in A_2$, recovering $P \in \phi^{-1}(Q)$ may be expensive.

We will rely on the efficient representation of isogenies of [Rob22a]. However, since it is only stated there for N-isogenies rather than for general β-isogenies (with β symmetric under the Rosatti involution and totally positive), we need to assume in this section that we can find a presentation $i_{A_2} \colon A_2 \times E_2^{m_2} \to E^{n_2}$ that is a product of N_j-isogenies $i_{A_2,j} \colon A_2 \times E^{m_{2,j}} \to E^{n_{2,j}}$. We say that such a presentation is admissible. For instance if we have a N_1-isogeny $A_2 \times E^{m_{2,1}} \to E^{n_{2,1}}$ and a N_2-isogeny $A_2 \times E^{m_{2,2}} \to E^{n_{2,2}}$, with N_1 prime to N_2, then we have an embedding $A_2 \times E^{m_{2,1}+m_{2,2}} \to E^{n_{2,1}+n_{2,2}}$. Extending [Rob22a] to β-isogenies is out of scope of this paper (but see [DJRV22]). So we will be content with the assumption above, and refer to [KNRR21, Theorem 2.16] for a precise description of when we can find such isogenies.

By the discussion above, we can evaluate the $i_{A_2,j}$ on the image of $\phi(A_1)$, so in particular on the $A_2[\ell]$ torsion for small primes ℓ prime to the degree of the $i_{A_2,j}$. We can also evaluate $i_{A_2,j}$ on the $E^{m_{2,j}}[\ell]$, since it will be given by a matrix of endomorphisms. By [Rob22a], this is enough to represent the $i_{A_2,j}$, hence the presentation $i_{A_2} \hookrightarrow E^{n_2}$.

3.4. **Similitude to isogeny.** Let $\psi \colon (M_1, H_1) \to (M_2, H_2)$ be a N-similitude between unimodular Hermitian R-modules. This time we do not assume N smooth. We would like to compute the associated N-isogeny $\phi \colon A_1 \to A_2$ between ppavs. We assume that we have an effective presentation for A_1.

Following a similar strategy in Deuring correspondence, such an isogeny could be computed in two steps:

(1) Find another N'-similitude $\psi' \colon (M_1, H_1) \to (M_2, H_2)$, with N' smooth and the N'-torsion accessible, and use Section 3.3 to evaluate the corresponding isogeny ϕ' (and if necessary find an effective presentation for A_2).
(2) We can now evaluate ϕ as follow. The map $\gamma = \phi \circ \tilde{\phi}'$ is an endomorphism of A_2, which can be lifted via presentation $i_{A_2} \colon A_2 \hookrightarrow E^{n_2}$ to an endomorphism of E^{n_2} via Lemma 3.5. Since γ can be efficiently evaluated, ϕ can be evaluated on the image of $\tilde{\phi}'$. In particular, ϕ can be evaluated on the ℓ-torsion (for small ℓ prime to N, N'), hence hence ϕ can be evaluated everywhere thanks to [Rob22a]. (An alternative approach which does not require a presentation

of A_2, is to instead use the presentation of A_1 to evaluate the endomorphism $\tilde{\phi} \circ \phi'$, hence find an efficient representation of $\tilde{\phi}$, hence find an efficient representation of ϕ, still by [Rob22a]).

In Section 5, we will explain how to smoothen the isogeny corresponding to an invertible ideal $\mathfrak{a} \to R$ by smoothening the embedded isogeny $\mathfrak{a} \oplus \overline{\mathfrak{a}} \to R \oplus R$, for $\mathfrak{a}$ an invertible R-ideal.

However, we probably cannot hope to get a general smoothening result as needed in Item 1 in the general case. Indeed, there is a first obstruction related to the conductor. For instance, if $\mathfrak{a}$ is the conductor ideal (or divides the conductor ideal), then the corresponding isogeny $E \to E_{\mathfrak{a}}$ is the going up isogeny. Any other isogeny $E \to E_{\mathfrak{a}}$ factorizes through this going up isogeny, so need to be of norm divisible by $\mathcal{N}(\mathfrak{a})$. At the level of ideals, this is seen from the fact that every element $x \in \mathfrak{a}$ is of norm $\mathcal{N}(x)$ divisible by $\mathcal{N}(\mathfrak{a})^2$. By the converse of Kani's lemma, any N-isogeny $F\colon E^2 \to E_{\mathfrak{a}}^2$ comes from an isogeny diamond. By the above remark, the component morphisms in dimension 1 are either 0 or of degree divisible by $\mathcal{N}(\mathfrak{a})$, so $\deg F$ is divisible by $\mathcal{N}(\mathfrak{a})$ too. We say that ψ is an horizontal isogeny if the orders appearing in Lemma 2.5 are the same for M_1 and M_2.

A second obstruction, even in the case that $A_1 = E^g$, is that we may have no N-similitude at all between (R^g, H_R^g) and (M, H_M), because of the arithmetic obstructions described in [KNRR21, Theorem 2.16]. This can be fixed, in the general case, by trying to find a smooth N-isogeny $A_1 \times E^m \to A_2 \times E^m$ (for the product polarisations) instead.

Open question: can we find an effective smoothening for an horizontal isogeny?

The main contribution of this paper is a positive answer to this question in the case of dimension 1 (by going to dimension 2); indeed in this case horizontal isogenies corresponds to invertible ideals.

Remark 3.12. By Lemma 2.5, the abelian variety $A = \mathcal{HOM}_R(M, E)$ is isomorphic to a product $A = \prod E_i$. Our solution in dimension 1 also gives a solution for horizontal isogenies in higher dimension when the principal polarisations are product of principal polarisations of dimension 1. But of course in general, a principal polarisation on A will not be a product polarisation.

3.5. **Abelian varieties to modules.** We can also look at the converse: translating from abelian varieties and isogenies to modules and module maps.

Given an abelian variety A, which we know is in the image of $\mathcal{HOM}_R(\cdot, E)$, can we find the torsion free module M representing A? In the case of dimension 1, the question boils down to finding from $E_{\mathfrak{a}}$ an ideal equivalent to $\mathfrak{a}$, so can be done in quantum subexponential time thanks to Kuperberg's algorithm.

Open question: Is there an abelian variety to module subexponential quantum algorithm in higher dimension? What if we suppose that we are also given some explicit R-endomorphisms on A, not induced by the R-orientation?

Another related question is finding an effective presentation $i_A\colon A \hookrightarrow E^n$ of A. If we know the module M corresponding to A, we can try to find as in Section 3.3 a presentation $R^n \twoheadrightarrow M$ given by a product of N_i-similitudes, and apply a smoothening step to compute the presentation as in Section 3.4.

Conversely, if we are given a full presentation $i_A\colon A \hookrightarrow E^n \to E^m$ of A, where the map $X\colon E^n \to E^m$ is given by any effective representations of isogenies, then it suffices to identify X as a matrix of endomorphisms to recover the map $R^m \to R^n$, hence the module M as the cokernel of this map. One way to do that is compute the norm and trace of the endomorphism γ, and distinguish between γ and $\overline{\gamma}$ by evaluating it on a point.

If we are only given $i_A\colon A \hookrightarrow E^n$, but not the map $E^n \to E^m$, we can try to construct it by looking at how matrix of endomorphisms of E acts on the image of $A[\ell]$ by i_A for small ℓ. This gives us a relation matrix on the morphisms $A \to E$ given by i_A. We could then use the fact that A is principally polarised to detect when we have found enough relations (via pairings).

We now look at the question of converting an isogeny $\phi\colon A_1 \to A_2$ into a module map $\psi\colon M_2 \to M_1$. The discussion of Section 3.2 handles the case of a "small" isogeny, and Section 3.3 handles the case of smooth isogenies as long as we can find effective accessible presentations of the intermediate abelian varieties.

For the general case, if we have effective presentations $A_1 \hookrightarrow E_1^{n_1}$ and $A_2 \hookrightarrow E_2^{n_2}$, we know by Lemma 3.5 that ϕ lifts to a map $\tilde{\phi}\colon E_1^{n_1} \to E_2^{n_2}$. If we can find an effective representation of $\tilde{\phi}$, we can

try to identify it as a matrix X of endomorphisms as in the question above; this gives a representation of the module map $\psi\colon M_2 \to M_1$.

Open question: can we find such a lift efficiently?

We remark that a similar problem is solved for the Deuring correspondence in [CII+23].

4. Hermitian forms and quaternions

Let F be a field of characteristic not 2.

Let K/F be a quadratic extension. We will denote $x \mapsto \overline{x}$ the nontrivial automorphism of K/F.

4.1. **Hermitian forms.** A *K/F-sesquilinear form* on a K-vector space V is a map

$$\langle\cdot,\cdot\rangle\colon V \times V \to K$$

such that

- $\langle\cdot,\cdot\rangle$ is F-bilinear,
- $\langle\cdot,\cdot\rangle$ is K-linear on the left, and
- $\langle v,u\rangle = \overline{\langle u,v\rangle}$ for all $u,v \in V$.

The associated *Hermitian form* is the map $H\colon V \to F$ defined by

$$H(v) = \langle v,v\rangle.$$

The sesquilinear form can be recovered from the Hermitian form by polarisation: if $i \in K$ is such that $i^2 = c \in F^\times$ and $K = F(i)$, then

$$\langle u,v\rangle = \frac{1}{4}\Big(H(u+v) - H(u-v) + \frac{i}{c}(H(iu+v) - H(iu-v))\Big).$$

A *similitude of multiplier* λ is a K-linear map $A\colon V \to V$ such that $H(Av) = \lambda H(v)$ for all v (equivalently, $\langle Au, Av\rangle = \lambda\langle u,v\rangle$ for all u,v). Write $\mathrm{GU}(H)$ the group of invertible similitudes. A *strict similitude* (nonstandard terminology, I don't know if there is a standard one) is a similitude A of multiplier $\det(A)$. Write $\mathrm{GU}'(H)$ the group of invertible strict similitudes. An *isometry* is a similitude of multiplier 1. Write $\mathrm{U}(H)$ the group of isometries. We have $\mathrm{GU}'(H) \cap \mathrm{U}(H) = \mathrm{SU}(H)$, the group of isometries of determinant 1.

We say that the sequilinear (or the Hermitian) form is *nondegenerate* if its left kernel is trivial.

From now on, all our vector spaces will be finite dimensional and all our forms will be nondegenerate.

For every K-linear map $V \to V$, there exists a unique K-linear map $A^*\colon V \to V$, the *adjoint of A*, such that

$$\langle Au, v\rangle = \langle u, A^*v\rangle \text{ for all } u,v.$$

We then also have

$$\langle u, Av\rangle = \langle A^*u, v\rangle \text{ for all } u,v,$$

and $(A^*)^* = A$. We have $\det A^* = \overline{\det A}$. We have

$$A \in \mathrm{GU}(H) \text{ of multiplier } \lambda \text{ iff } A^*A = \lambda\,\mathrm{Id} \text{ iff } AA^* = \lambda\,\mathrm{Id}\,.$$

In particular, a similitude A of multiplier λ satisfies

$$\mathcal{N}_{K/F}(\det A) = \lambda^2, \text{ i.e. } \mathcal{N}_{K/F}(\lambda^{-1}\det A) = 1.$$

By Hilbert 90 we then have $\lambda^{-1}\det A = \mu^{-1}\overline{\mu}$ for some $\mu \in K^\times$, and therefore μA is a strict similitude. We therefore have

$$\mathrm{GU}(H) = K^\times \cdot \mathrm{GU}'(H)$$

(and $\mathrm{GU}'(H) \cap K^\times = F^\times$).

Let $d \in F^\times$ and $V = K^2$ equipped with the Hermitian form

$$H((x,y)) = x\overline{x} - dy\overline{y}.$$

Then the adjoint of a 2×2 matrix acting on V is given by

$$\begin{pmatrix} x & z \\ y & t \end{pmatrix}^* = \begin{pmatrix} \overline{x} & -d\overline{y} \\ -\overline{z}/d & \overline{t} \end{pmatrix}.$$

4.2. **Quaternion algebras.** A *quaternion algebra* over F is an F-algebra with basis $1, i, j, ij$ satisfying

$$i^2 = c,\ j^2 = d,\ ij = -ji \text{ for some } c, d \in F^\times.$$

Such an algebra $B = \left(\frac{c,d}{F}\right)$ has a unique F-linear involution $b \mapsto \overline{b}$ such that

- $\overline{\overline{b}} = b$ for all $b \in B$,
- $\overline{bb'} = \overline{b'}\,\overline{b}$ for all $b, b' \in B$,
- $\overline{i} = -i$, and
- $\overline{j} = -j$.

The *reduced trace* $\mathrm{trd}\colon B \to F$ is defined by $\mathrm{trd}(b) = b + \overline{b}$. The *reduced norm* $\mathrm{nrd}\colon B \to F$ is defined by $\mathrm{nrd}(b) = b\overline{b} = \overline{b}b$ and is multiplicative.

The matrix algebra $M_2(F)$ is a quaternion algebra over F, and we write the corresponding quaternionic involution $M \mapsto \tilde{M}$ (to avoid confusion with application of $\bar{\cdot}$ to the coefficients):

$$\widetilde{\begin{pmatrix} x & z \\ y & t \end{pmatrix}} = \begin{pmatrix} t & -z \\ -y & x \end{pmatrix}.$$

The reduced trace is the usual trace of matrices, and the reduced norm is the usual determinant of matrices.

Assume $c \notin (F^\times)^2$ and let $K = F(i) \subset B$. The quaternionic involution induces Galois conjugation on K. Right multiplication by K gives B the structure of a 2-dimensional K-vector space with basis $(1, j)$:

$$B = K + jK.$$

Left multiplication by B induces an injective morphism of F-algebras $\Phi\colon B \hookrightarrow \mathrm{End}_K(B) \cong M_2(K)$ given by

$$\Phi\colon x + jy \mapsto \begin{pmatrix} x & d\overline{y} \\ y & \overline{x} \end{pmatrix} \text{ for } x, y \in K.$$

The reduced norm is a Hermitian form on the K-vector space B:

$$\mathrm{nrd}(x + jy) = x\overline{x} - dy\overline{y} \text{ for } x, y \in K.$$

We have $\Phi(b)^* = \Phi(\overline{b}) = \widetilde{\Phi(b)}$ for all $b \in B$, and in fact for all $M \in M_2(K)$, we have $M \in \Phi(B)$ if and only if $M^* = \tilde{M}$ (and in that case $M = \Phi(b)$ with $b = M(1)$).

Since for all $b \in B$, $\Phi(b)\Phi(b)^* = \Phi(b\overline{b}) = \Phi(\mathrm{nrd}(b)) = \det \Phi(b)$, the map Φ induces a group homomorphism

$$\Phi\colon B^\times \to \mathrm{GU}'(\mathrm{nrd}),$$

and this map is an isomorphism: if $MM^* = \det(M)\,\mathrm{Id}$ and M is invertible, then $MM^* = M\tilde{M}$ so $M^* = \tilde{M}$ and $M \in \Phi(B^\times)$ as claimed.

Reformulating, we get:

Lemma 4.1. *An element $b \in B^\times$ is a $\mathrm{nrd}(b)$-similitude for the norm form on B; it induces a $\mathrm{nrd}(b)$-strict similitude $\Phi(b)$ on $K \oplus K$ (for the product norm form on each copy of K).*

5. Computing the ideal group action

Let $\mathfrak{a}$ be an invertible ideal. Via our equivalence of categories, we need to compute the isogeny corresponding to the inclusion of $\mathfrak{a} \to R$ which is an $N = \mathcal{N}(\mathfrak{a})$-isogeny. In particular, the principal Hermitian form on $\mathfrak{a}$ is $H_R/\mathcal{N}(\mathfrak{a})$ by Example 2.14.

We try instead to build a dimension 2 isogeny corresponding $\mathfrak{a} \oplus \overline{\mathfrak{a}} \to R \oplus R$ (orthogonal sum). Rather than computing the corresponding isogeny, we can use any equivalent isogeny. We thus look for a unimodular module equivalent to $\mathfrak{a} \oplus \overline{\mathfrak{a}}$.

Let $R = \mathbb{Z}[\delta]$, and consider the quaternion order $\mathcal{O} = \mathbb{Z}[i, j, ij]$ with $i^2 = -1$, $j = \delta$.

Lemma 5.1. *Let H_R be the canonical Hermitian form on R given by the norm $H_R(x) = \mathcal{N}(x) = x\overline{x}$, and $H_\mathcal{O}$ the canonical R-Hermitian form on $\mathcal{O}$ given by the quaternionic norm $H_\mathcal{O}(x) = \mathcal{N}(x) = x\overline{x}$. Let $\mathcal{I} = \mathfrak{a} \oplus i\overline{\mathfrak{a}}$ The Hermitian module $(\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \oplus (\overline{\mathfrak{a}}, H_R/\mathcal{N}(\mathfrak{a}))$ is equivalent to the Hermitian module $(\mathcal{I}, H_\mathcal{O}/\operatorname{nrd}(\mathcal{I}))$.*

Proof. The order $\mathcal{O}$ is a rank 2 free R-module, and via this identification, by Section 4.2, since $i^2 = -1$, the form $H_\mathcal{O}$ is the Hermitian form $H_R \oplus H_R$. Since $\operatorname{nrd}(\mathcal{I}) = \mathcal{N}(\mathfrak{a})$, the conclusion follows. □

Proposition 5.2. *Let $\mathcal{I} \subset \mathcal{O}$ be as above. Let $\mathcal{J}$ be an $\mathcal{O}$-ideal equivalent to $\mathcal{I}$: $\mathcal{J} = \beta\mathcal{I}$ for some $\beta \in \mathcal{O} \otimes \mathbb{Q}$. Then β induces a morphism $\beta\colon \mathcal{I} \to \mathcal{J} \subset \mathcal{O}$, which is a $\operatorname{nrd}(\mathcal{J})$-similitude for the $\mathcal{O}$-Hermitian modules $(\mathcal{I}, H_\mathcal{O}/\operatorname{nrd}(\mathcal{I})) \to (\mathcal{O}, H_\mathcal{O}))$, and $\Phi(\beta)$ (where Φ is defined in Section 4.2) induces a $\operatorname{nrd}(\mathcal{J})$-similitude for the R-Hermitian modules $(\mathfrak{a}, H_R/\mathcal{N}(\mathfrak{a})) \oplus (\overline{\mathfrak{a}}, H_R/\mathcal{N}(\mathfrak{a})) \to (R, H_R) \oplus (R, H_R)$.*

Proof. The same reasoning as in Example 2.14 shows that β is an $\operatorname{nrd}(\mathcal{J})$-similitude, so $\Phi(\beta)$ is a $\operatorname{nrd}(\mathcal{J})$-similitude too by Lemma 4.1. □

We have thus reduced our smoothening problem from a rank 2 R-module to a rank 1 $\mathcal{O}$-module. For any N' large enough ($N' = O(\Delta_R^3)$), applying KLPT gives a morphism $\beta\colon \mathcal{I} \to \mathcal{J} \subset \mathcal{O}$. (The order $\mathcal{O}$ is not necessarily a maximal quaternion order, but KLPT still applies with only minimal adaptations.)

TODO insert here adapted KLPT.

By Proposition 5.2, this morphism corresponds to an N'-similitude of Hermitian modules, hence an N'-isogeny of principally polarised abelian surfaces: $E^2 \to E/\mathfrak{a} \times E/\overline{\mathfrak{a}}$. [Aurel : Notation? $E_\mathfrak{a}$? $E/E[\mathfrak{a}]$?]

The KLPT algorithm is heuristic, for a proven polynomial time algorithm under GRH (but with a worse bound), we refer to [Wes22].

We compute the kernel of this isogeny using Section 3: let $R^4 \twoheadrightarrow \mathcal{I}$ be a surjection, composing with the map β above, we get a morphism $R^4 \to \mathcal{I} \to \mathcal{O} \simeq R^2$, hence a 4×2 matrix X. Passing to abelian varieties, we have a morphism $F\colon E^2 \to E^4$, whose image is precisely $E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}}$; since the matrix X is explicit, we can recover the kernel of F and evaluate it as a N'-isogeny.

It remains to distinguish between $E_\mathfrak{a}$ and $E_{\overline{\mathfrak{a}}}$. Since we have an N'-isogeny $F\colon E^2 \to E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}}$, we can also compute its contragredient isogeny $\tilde{F}$, and compute $\gamma' = \tilde{F} \circ \gamma \circ F\colon E^2 \to E^2$, where γ acts by -1 on one of our unknown curve and by 1 on the other. Evaluating γ' and comparing with the matrix we were supposed to get, allows us to identify which curve is which. An alternative (simpler) method is to use pairings to compute the degree of the two individual isogenies from $E \to E_\mathfrak{a}$, and the two isogenies $E \to E_{\overline{\mathfrak{a}}}$ and distinguish the two codomain.

We remark that we can also evaluate the inclusion map $E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}} \to E^4$ on points prime to N' by going through $E^2 \to E^4$; by [Rob22a] this is enough to reconstitute the individual isogenies $E_\mathfrak{a} \to E$ and $E_{\overline{\mathfrak{a}}} \to E$ (given by projection from E^4).

Theorem 5.3. *Computing the action by $\mathfrak{a}$ can be done by evaluating a N'-isogeny $F\colon E^2 \to E/\mathfrak{a} \times E/\overline{\mathfrak{a}}$ in dimension 2, where N' can be taken to be powersmooth of norm $\left(\Delta_R \min(\sqrt{\Delta_R}, \mathcal{N}(\mathfrak{a}))\right)^2$. The kernel of F can be recovered from evaluating the action of R on $E[N']$ and some pairings + DLPs. Using a powersmooth bound of $O(\log(\Delta))$ for N', the corresponding isogeny in dimension 2 can then be evaluated in $O(\log^8(\Delta_R))$ arithmetic operations.*

Proof. The complexity of the isogeny is given by [Rob22b, Proposition 2.9 and Corollary 2.10]. □

Example 5.4. We have implemented in Pari/GP our algorithm to find an equivalent isogeny $F\colon E^2 \to E/\mathfrak{a} \times E/\overline{\mathfrak{a}}$ which is an N-isogeny with N powersmooth in a CSIDH setting over $\mathbb{F}_p$ with p a prime number of around 1024 bits. We note that for this size of primes, computing the lattice of relations of the corresponding class group is completely out of reach. We take a random (split) prime ideal $\mathfrak{a}$ of norm 512 bits (which is the approximate size of the class group). Our non optimised KLPT implementation finds on average in less than 1s a powersmooth equivalent isogeny with average smoothness bound of 2586. The code is available at TODO.

Using the results of Section 3 to compute the corresponding powersmooth isogeny remains a work in progress. However, an old unpublished "record computation" from 2010 which used AVIsogenies [BCR10] to compute a 1321-isogeny in dimension 2 (so an isogeny of degree 1745041) took around 5h

back then. Although the state of the art of isogeny computation in higher dimension has improved somewhat since, this computation was specifically done on an example where the 1321-torsion was rational; in our class group application we will need in general to work over an extension. So although we have a general polynomial time algorithm, we cannot hope to have an efficient algorithm. However, by carefully selecting the parameters (so that we have many accessible torsion), it is plausible that we may find practical instances (the situation is very similar to making the Deuring correspondence from polynomial time to effective). We refer to Section 7 for more details and to Appendix A for an explicit example.

Example 5.5 (An elementary description of Clapotis)**.** As explained in Section 1, the powersmooth isogeny $E^2 \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$ that we construct using our equivalence of categories Section 2 with Hermitian R-modules, can also be described as follows as the isogeny attached by Kani's lemma to an isogeny diamond.

Given $R = \mathbb{Z}[\delta]$ and an invertible ideal $\mathfrak{a} \subset R$, construct as above the quaternion order $\mathcal{O} = \mathbb{Z}[i, j, ij]$ with $i^2 = -1$, $j = \delta$, and the ideal $\mathcal{I} = \mathfrak{a} \oplus i\overline{\mathfrak{a}}$ of $\mathcal{O}$ of reduced norm $\operatorname{nrd}(\mathcal{I}) = \mathcal{N}(\mathfrak{a})$. Find a smoothening integral ideal $\mathcal{J} = \beta\mathcal{I}$ of $\mathcal{I}$ of reduced norm N (e.g. via an adapted version of KLPT). Since $\mathcal{J}$ is integral, $\beta = \overline{\gamma}/\operatorname{nrd}(\mathcal{I})$ for some element $\gamma \in \mathcal{I}$ of reduced norm $\operatorname{nrd}(\gamma) = N \operatorname{nrd}(\mathcal{I})$. Write $\gamma = x + iy$, with $x \in \mathfrak{a}$ and $y \in \overline{\mathfrak{a}}$. We have $\operatorname{nrd}(\gamma) = \gamma\overline{\gamma} = x\overline{x} + y\overline{y} = \mathcal{N}(x) + \mathcal{N}(y) = N\mathcal{N}(\mathfrak{a})$.

To the element x, we can attach as in Example 2.14 the isogeny $\phi_{\mathfrak{b}} \colon E \to E_{\mathfrak{a}}$ corresponding to the ideal $\mathfrak{b} \coloneqq \overline{x}/\mathcal{N}(\mathfrak{a})\mathfrak{a}$, isogeny of degree $\mathcal{N}(\mathfrak{b}) = \mathcal{N}(x)/\mathcal{N}(\mathfrak{a})$, and whose kernel is $E[\mathfrak{b}]$. The endomorphism $\overline{x}\overline{y}$ is divisible by $\mathcal{N}(\mathfrak{a})$, and $\overline{x}\overline{y}/\mathcal{N}(\mathfrak{a}) \in \mathfrak{b}$ so the endomorphism $\overline{x}\overline{y}/\mathcal{N}(\mathfrak{a})$ of norm $\mathcal{N}(x)/\mathcal{N}(\mathfrak{a}) \times \mathcal{N}(y)/\mathcal{N}(\mathfrak{b})$ factorizes as $E \to E_{\mathfrak{a}} \to E$, a $\mathcal{N}(x)/\mathcal{N}(\mathfrak{a})$-isogeny followed by a $\mathcal{N}(y)/\mathcal{N}(\mathfrak{a})$ isogeny.

Applying the same factorization to the element y, we get that $\overline{x}\overline{y}/\mathcal{N}(\mathfrak{a})$ factorizes as $E \to E_{\overline{\mathfrak{a}}} \to E$, a $\mathcal{N}(y)/\mathcal{N}(\mathfrak{a})$-isogeny followed by a $\mathcal{N}(x)/\mathcal{N}(\mathfrak{a})$ isogeny.

We thus have an isogeny diamond, hence by Kani's lemma an isogeny $F \colon E \times E \to E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}}$ which is a $(\mathcal{N}(x) + \mathcal{N}(y))/\mathcal{N}(\mathfrak{a}) = N$-isogeny. If $\mathcal{N}(x)/\mathcal{N}(\mathfrak{a})$ is prime to $\mathcal{N}(y)/\mathcal{N}(\mathfrak{a})$, the kernel of F is simply given by $(\mathcal{N}(x)/\mathcal{N}(\mathfrak{a})P, \overline{x}\overline{y}P)$ for $P \in E[N]$.

The general case can be treated as in Section 3. We refer to [PR23] or the appendix for a self contained treatment of this elementary approach.

6. Applications

The main application is of course signatures and zero knowledge proofs of oriented isogenies. We refer to [BDGP23] for a nice survey on existing signatures and ZK-schemes. The main difference of Clapotis with a signature scheme like SeaSign [DG19] which is also polynomial time, is that like CSI-Fish [BKV19] we are able to prove knowledge of an isogeny corresponding to an arbitrary ideal $\mathfrak{a}$, whereas SeaSign can only prove knowledge of a random ideal sampled as $\mathfrak{a} = \prod \mathfrak{a}_i^{e_i}$ with small ideals $\mathfrak{a}_i$ and exponents e_i.

We discuss a second application about computing an isogeny with known generator kernel. Assume that $E/\mathbb{F}_q$ is an ordinary curve, or a supersingular curve defined over $k = \mathbb{F}_p$. If $K = \langle T \rangle \subset E/\mathbb{F}_q$ is generated by a rational generator $T \in E(\mathbb{F}_q)$ of order N, and K corresponds to an horizontal isogeny (for instance this is automatically the case if $\mu_N \cap \mathbb{F}_q = 1$), then, assuming the factorisation of N is known, we can apply Section 5 to compute the isogeny $\phi \colon E \to E/K$ in polynomial time in $\log q$.

Indeed, we need to compute the ideal $\mathfrak{a} \subset \operatorname{End}(E)$ corresponding to K. We can compute $\mathbb{Z}[\pi] \subset \operatorname{End}_k(E)$ in polynomial time by point counting, and since we know the factorisation of N, we can find in polynomial time the N-primary part of the conductor of $\operatorname{End}_k(E)$ using [Rob22b]. In particular we get the order $\mathbb{Z}[\pi] \subset R \subset \operatorname{End}_k(E)$ such that the index $[\operatorname{End}_k(E) : R]$ is prime to N; this is enough to apply the methods of Section 5, as long as we are careful to use isogenies of degree prime to the conductor f of R in $\operatorname{End}_k(E)$.

For each prime $\ell \mid N$, we know that $\ell = \ell_1\ell_2$ splits in R, and compute which of the two prime ideal is zero on $(\ell/\ell_i)T$. If $N = \ell^e N'$, then $(\mathfrak{a}, \ell^e) \cap R = \ell_i^e$. This allows us to recover $\mathfrak{a} \cap R$, and then we can apply Section 5.

7. Perspectives

Although we have a polynomial time algorithm to compute the ideal class group action, the bound of Theorem 5.3 is rather impractical. However, it is probably that by selecting appropriate primes p, especially ones with large easily accessible 2^n or 3^m-torsion, we can make the algorithm much more practical, especially when combined with the ideas of splitting the isogeny in several blocks using Section 3.

Our technique in Section 5 to compute the class group action is to reduce to KLPT. There is a lot of literature in making the Deuring correspondence practical [DKLPW20; DLLW23; DLRW23; EPSV23]. Cleary all these techniques (selecting a nice "SQISign" prime, refreshing the torsion with an endomorphism when splitting the isogeny in blocks) could extend to our settings. We hope that by appropriately selecting parameters, we will be able to make the CSIDH group action not only polynomial time, but also practical.

While our equivalence of categories applies to non invertible ideal, our algorithm to find a suitable isogeny in dimension 2 requires the ideal $\mathfrak{a}$ to be invertible. In particular, it does not apply to the conductor ideal of R (see Section 3.4), hence we do not have a polynomial algorithm to climb in the volcano when the conductor is divisible by a large prime number. There thus seems to be a strong algorithmic gap between computing horizontal ideal isogenies and vertical ones. In fact, the module representation can only describe horizontal or ascending isogenies, so descending the volcano cannot be described by an ideal. So moving vertically efficiently in the volcano will require new ideas.

More generally, we hope that the results of Section 2 will help develop higher dimensional isogeny based cryptography beyond simply using Kani's lemma. Using a similar method as in Section 5, it might also be possible to improve the bounds on the KLPT algorithm by going to higher dimension, using the equivalence of categories described in [JKP+18] (see Remark 2.10).

References

[ACL+22] S. Arpin, M. Chen, K. E. Lauter, R. Scheidler, K. E. Stange, and H. T. Tran. "Orientations and cycles in supersingular isogeny graphs". In: *arXiv preprint arXiv:2205.03976* (2022) (cit. on p. 8).

[BDD+24] A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. "SQIsign2D-West: The Fast, the Small, and the Safer". May 2024. eprint: 2024/760. (Cit. on p. 4).

[BDGP23] W. Beullens, L. De Feo, S. D. Galbraith, and C. Petit. "Proving knowledge of isogenies: a survey". In: *Designs, Codes and Cryptography* (2023), pp. 1–32 (cit. on p. 17).

[BKV19] W. Beullens, T. Kleinjung, and F. Vercauteren. "CSI-FiSh: efficient isogeny based signatures through class group computations". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2019, pp. 227–247 (cit. on pp. 1, 17).

[BCR10] G. Bisson, R. Cosset, and D. Robert. *AVIsogenies*. Magma package devoted to the computation of isogenies between abelian varieties. 2010. URL: https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000). Latest version 0.7, released on 2021-03-13. (Cit. on p. 16).

[CD23] W. Castryck and T. Decru. "An efficient key recovery attack on SIDH". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 423–447 (cit. on p. 3).

[CLMPR18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: an efficient post-quantum commutative group action". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)*. Springer. 2018, pp. 395–427 (cit. on p. 2).

[CII+23] M. Chen, M. Imran, G. Ivanyos, P. Kutas, A. Leroux, and C. Petit. "Hidden Stabilizers, the Isogeny To Endomorphism Ring Problem and the Cryptanalysis of pSIDH". In: *arXiv preprint arXiv:2305.19897* (2023) (cit. on p. 14).

[CL23] M. Chen and A. Leroux. "SCALLOP-HD: group action from 2-dimensional isogenies". In: *Cryptology ePrint Archive* (2023) (cit. on p. 1).

[CK20] L. Colò and D. Kohel. "Orienting supersingular isogeny graphs". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 414–437 (cit. on p. 7).

[DLRW23] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". Mar. 2023. eprint: 2023/436. (Cit. on p. 18).

[DG19] L. De Feo and S. D. Galbraith. "SeaSign: compact isogeny signatures from class group actions". In: *Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38*. Springer. 2019, pp. 759–789 (cit. on p. 17).

[DKLPW20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. "SQISign: compact post-quantum signatures from quaternions and isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2020)*. Springer. 2020, pp. 64–93 (cit. on p. 18).

[DLLW23] L. De Feo, A. Leroux, P. Longa, and B. Wesolowski. "New algorithms for the Deuring correspondence: towards practical and secure SQISign signatures". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 659–690 (cit. on p. 18).

[DJRV22] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". In: *Moscow Mathematical Journal* 22 (Feb. 2022), pp. 613–655. HAL: hal-01629829. (Cit. on p. 12).

[EPSV23] J. K. Eriksen, L. Panny, J. Sotáková, and M. Veroni. "Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic". In: *Cryptology ePrint Archive* (2023) (cit. on p. 18).

[FFK+23] L. D. Feo, T. B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny, and B. Wesolowski. "SCALLOP: scaling the CSI-FiSh". In: *IACR International Conference on Public-Key Cryptography*. Springer. 2023, pp. 345–375 (cit. on p. 1).

[JKP+18] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate. "Abelian varieties isogenous to a power of an elliptic curve". In: *Compositio Mathematica* 154.5 (2018), pp. 934–959 (cit. on pp. 2, 4–8, 18).

[Kan11] E. Kani. "Products of CM elliptic curves". In: *Collectanea mathematica* 62.3 (2011), pp. 297–339 (cit. on pp. 2, 4, 6).

[KNRR21] M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "Spanning the isogeny class of a power of an elliptic curve". In: *Mathematics of Computation* 91.333 (Sept. 2021), pp. 401–449. DOI: 10.1090/mcom/3672 (cit. on pp. 2–4, 8–10, 12, 13).

[KLPT14] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. "On the quaternion-isogeny path problem". In: *LMS Journal of Computation and Mathematics* 17.A (2014), pp. 418–432 (cit. on pp. 2, 3).

[Ler22] A. Leroux. "Quaternion algebras and isogeny-based cryptography ". PhD thesis. LIX, 2022 (cit. on p. 8).

[LR22] D. Lubicz and D. Robert. "Fast change of level and applications to isogenies". In: *Research in Number Theory (ANTS XV Conference)* 9.1 (Dec. 2022). DOI: 10.1007/s40993-022-00407-9. HAL: hal-03738315. (Cit. on p. 12).

[MMPPW23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. "A direct key recovery attack on SIDH". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 448–471 (cit. on p. 3).

[NO23] K. Nakagawa and H. Onuki. "QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras". In: *Cryptology ePrint Archive* (2023) (cit. on pp. 2, 4).

[Oda69] T. Oda. "The first de Rham cohomology group and Dieudonné modules". In: *Annales scientifiques de l'École Normale Supérieure*. Vol. 2. 1. 1969, pp. 63–135 (cit. on p. 7).

[Onu21] H. Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields and Their Applications* 69 (2021), p. 101777 (cit. on p. 7).

[PR23] A. Page and D. Robert. "Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time". Nov. 2023. eprint: 2023/1766. (Cit. on pp. 2–4, 17).

[Rob22a] D. Robert. "Evaluating isogenies in polylogarithmic time". Aug. 2022. eprint: 2022/1068, HAL: hal-03943970. (Cit. on pp. 10, 12, 13, 16).

[Rob22b] D. Robert. "Some applications of higher dimensional isogenies to elliptic curves (overview of results)". Dec. 2022. eprint: 2022/1704, HAL: hal-03943973. (Cit. on pp. 10, 16, 17).

[Rob23] D. Robert. "Breaking SIDH in polynomial time". In: *Eurocrypt 2023* (Apr. 2023) (cit. on p. 3).

[Rob24a] D. Robert. "From ideals to modules for isogeny based cryptography". Leuven isogeny days 5, Leuven. Sept. 2024. URL: http://www.normalesup.org/~robert/pro/publications/slides/2024-09-Leuven.pdf (cit. on p. 4).

[Rob24b] D. Robert. "On the efficient representation of isogenies (a survey)". June 2024. eprint: 2024/1071. (Cit. on p. 2).

[Voi21] J. Voight. *Quaternion algebras*. Springer Nature, 2021 (cit. on p. 8).

[Wat69] W. Waterhouse. "Abelian varieties over finite fields". In: *Ann. Sci. Ecole Norm. Sup* 2.4 (1969), pp. 521–560 (cit. on pp. 2, 4, 6).

[Wes22] B. Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 1100–1111 (cit. on pp. 3, 16).

Appendix A. An explicit example

We work with a quadratic order $R = \mathbb{Z}[\delta]$, with discriminant $\Delta_R = -pq$, with

$$p = 693097151489577169008672217912084052214809976903253232857439$$

,

$$q = 144014279945332992600667304141689749681556179039441260721799 9$$

two large primes of around 200 bits.

We take a random prime ideal of norm around 2^{100},

$$\mathfrak{a} = (1186892866599125331799827393043, \delta + 562463914750828188674631388488).$$

We find the corresponding N'-similitude $(R \oplus R, H_R \oplus H_R) \to (\mathfrak{a} \oplus \overline{\mathfrak{a}}, 1/\mathcal{N}(\mathfrak{a})(H_R \oplus H_R)$:

$$\begin{pmatrix} a_1 & a_2 \\ \overline{a}_2 & -\overline{a}_1 \end{pmatrix}$$

with

$a_1 = 730594377336378409258208129615094829324651597292118719029127132479947334614738396732690462773929709811310289562069071998 48\delta +$
$239138920366495643822436943904896735642540491010143844930656444899207383116259620297039498968810541239735635138084059477053560711057268511 7$
$a_2 = 114155504161919358119344632422213146022144428116077667107470114109708474263601497365460072137180639005673846382636237257276 02\delta -$
$387659205644547192157915897414205420630533588822373999565979849161300384020793015572121919703684564680400468276590637565187124420599258998 7$

which is B-powersmooth with $B = 827$.

[Aurel : TODO ajouter la note CLAPOTI en appendice ?]

Email address: aurel.page@inria.fr

Email address: damien.robert@inria.fr

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE